TRANSMITTAL OF APPEAL BRIEF

Docket No.
SON-1710

In re Application of: Yoshihiro TSUKAMURA et al.

Application No.	Filing Date	Examiner	Group Art Unit
09/466,965	December 20, 1999	T. Tran	2134

Invention: AUTHENTICATION SYSTEM, FINGERPRINT IDENTIFICATION UNIT, AND AUTHENTICATION METHOD

TO THE COMMISSIONER OF PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed: July 14, 2004 .

The fee for filing this Appeal Brief is 330.00 .

[X] Large Entity [ ] Small Entity

[ ] A check in the amount of _____ is enclosed.

[X] Charge the amount of the fee to Deposit Account No. 18-0013 .
This sheet is submitted in duplicate.

[ ] Payment by credit card. Form PTO-2038 is attached.

[X] The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. 18-0013 .
This sheet is submitted in duplicate.

Dated: September 1, 2004

Ronald P. Kananen
Attorney Reg. No.: 24,104

RADER, FISHMAN & GRAUER PLLC
1233 20th Street, N.W.
Suite 501
Washington, DC 20036
(202) 955-3750
Customer No. 23353

PTO/SB/17 (10-03)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 330.00

Complete if Known	
Application Number	09/466,965
Filing Date	December 20, 1999
First Named Inventor	Yoshihiro Tsukamura
Examiner Name	T. Tran
Art Unit	2134
Attorney Docket No.	SON-1710

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit Card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 18-0013

Deposit Account Name: Rader, Fishman & Grauer PLLC

The Director is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 0.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below		Fee Paid
Total Claims	10	-20** =		x		=	
Independent Claims	3	-3** =		x		=	
Multiple Dependent						=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge – late filing fee or oath	
1052	50	2052	25	Surcharge – late provisional filing fee or cover sheet.	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	330.00
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive – unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	
Other fee (specify)					

*Reduced by Basic Filing Fee Paid **SUBTOTAL (3)** ($) 330.00

SUBMITTED BY				(Complete *(if applicable)*)	
Name (Print/Type)	Ronald P. Kananen	*Registration No. (Attorney/Agent)*	24,104	*Telephone*	(202) 955-3750
Signature				*Date*	September 1, 2004

DC166775

SON-1710
(80001-1710)

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Yoshihiro TSUKAMURA et al.

Examiner: T. Tran

Application No.: 09/466,965

Art Unit: 2134

Filed: December 20, 1999

Confirmation No.: 1790

For: AUTHENTICATION SYSTEM, FINGERPRINT IDENTIFICATION UNIT, AND AUTHENTICATION METHOD

APPELLANT'S BRIEF

MS APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This brief is in furtherance of the Notice of Appeal filed in the aforementioned application on July 14, 2004.

The fees required under § 1.17(f) and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate.

This brief contains items under the following headings as required by 37 C.F.R. § 1.192 and M.P.E.P. § 1206:

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is Sony Corporation of Tokyo, Japan ("Sony"). An assignment of all rights in the present application to Sony was executed by the inventor and recorded by the U.S. Patent and Trademark Office on **reel 01650** at **frame 0725**.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Total Number of Claims in Application

There are 10 claims pending in application.

Current Status of Claims

Claims canceled: 3, 6-8, 12-16

Claims withdrawn from consideration but not canceled: None

Claims pending: 1, 2, 4, 5, 9-11, and 17-19

Claims allowed: None

Claims rejected: 1, 2, 4, 5, 9-11, and 17-19

Claims On Appeal

The claims on appeal are claims 1, 2, 4, 5, 9-11, and 17-19

IV. STATUS OF AMENDMENTS

On December 20, 1999, Appellant filed a Preliminary Amendment to amend the specification so that the invention was more appropriately described. On November 4, 2003, each of claims 1 and 9 were amended to recite the storage-information recording means stores a private key generated by the public-key encryption method, and the user's instruction is one of a decryption of an encrypted text and an encryption of plain text, and the user's instruction is sent to the host computer through communication cable. Moreover, claims 2, 4, and 10 were amended to improve form. Claims 5 and 11 were amended to recite the encrypted text is received from the host computer and decrypted plain text is sent to the host

computer. On March 30, 2004, Appellant filed an Amendment After Final Rejection ("Amendment After Final"). In the Amendment After Final, Appellant attempted to amend each of claims 1 and 9 to recite that the processing control means accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the user's instruction specifies a decryption of an encrypted text, and the processing control means generates a symmetric key and a public key to encrypt the symmetric key when the user's instruction specifies an encryption of plain text. In response to the Amendment After Final, the Examiner issued an Advisory Action dated April 21, 2004 (Paper No. 11) refusing to enter the Amendment After Final. Appellant then filed a Request for Continued Examination (RCE) on April 23, 2004 so that the Amendment After Final could be entered. Following the filing of the RCE, the Examiner issued an improper first action final rejection of all pending claims that are the subject of this appeal.

Accordingly, the claims enclosed herein as Appendix A incorporate the amendments indicated in the Amendment After Final filed by Applicant on March 30, 2004.

V. SUMMARY OF INVENTION

Independent claim 1 recites an authentication system used when stored information is manipulated, comprising a host computer 200 comprising input means for inputting a user's instruction; command output means for generating from the user's instruction an instruction command which requests a predetermined processing to be executed and for outputting the instruction command; and communication means for communicating with an external unit; and a fingerprint identification apparatus 100 comprising communication means 160 for communicating with said host computer 200; processing control means 150 for executing a predetermined processing according to the instruction command input from said host computer 200 by said communication means 160; fingerprint detection means (111, 112, 113, 114) for detecting a fingerprint and for generating fingerprint data; storage-information recording means 140 for recording the fingerprint data and storage information related to the fingerprint data; and fingerprint identification means 120 for verifying fingerprint data detected by said fingerprint detection means (111, 112, 113, 114) with the fingerprint data recorded by said storage-information recording means 140, wherein said storage-information recording means 140 stores a private key generated by the public-key encryption method (p. 19, lines 9-13), wherein said processing control means 150 accesses the generated private

key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the user's instruction specifies a decryption of an encrypted text (p. 19, lines 1-18), wherein said processing control means 150 generates a symmetric key and a public key to encrypt the symmetric key when the user's instruction specifies an encryption of plain text (p. 20, lines 4-24), and wherein the user's instruction is sent to the host computer 200 through communication cable 300.

Independent claim 9 recites an authentication method used when stored information is manipulated, comprising the steps of a host computer 200 informing a user of a fingerprint-identification request according to a user's instruction and issuing a fingerprint-identification instruction command to a fingerprint identification apparatus (S11; p. 16 line 22 through p. 17, line 2); the fingerprint identification apparatus 120 reading a fingerprint after the user places a finger on the fingerprint identification apparatus (S12; p. 17, lines 2-6), verifying the read fingerprint with a stored fingerprint (S13; p. 17, lines 7-9), and sending a fingerprint-identification result to the host computer (S13; p. 17, lines 12-15); the host computer 200 allowing the user to specify the next instruction when the result is affirmative (p 17, lines 15-17), and issuing the instruction command corresponding to the next instruction; and the fingerprint identification apparatus accessing storage information according to the instruction command and executing a predetermined processing (p. 17, lines 17-21), wherein said storage-information recording means stores a private key generated by the public-key encryption method, and wherein the fingerprint identification apparatus accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the instruction command specifies a decryption of an encrypted text (p. 19, lines 1-18), wherein the fingerprint identification apparatus generates a symmetric key and a public key to encrypt the symmetric key when the instruction command is one that specifies an encryption of plain text (p. 20, lines 4-24), and wherein the instruction command is sent to the host computer through communication cable (p. 17, lines 12-15).

Independent claim 17 recites a fingerprint identification apparatus in an authentication system used when stored information is manipulated, comprising communication means 160 for communicating with a host computer 200; processing control means 150 for executing a predetermined processing according to an instruction command input from the host computer 200 by said communication means 160; fingerprint detection means (111, 112, 113, 114) for

detecting a fingerprint and for generating fingerprint data; storage-information recording means 140 for recording the fingerprint data and storage information related to the fingerprint data; and fingerprint identification means 120 for verifying fingerprint data detected by said fingerprint detection means (111, 112, 113, 114) with the fingerprint data recorded by said storage-information recording means 140.

The fingerprint apparatus and method recited in claims 1 and 9 detects and verifies a user's fingerprint with stored fingerprint data based on a user's instruction (S12, S13). When the user's detected fingerprint is verified successfully and the user's instruction requests the decryption of an encrypted text a processing controller of the apparatus accesses a private key stored in a recording means, decrypts a symmetric key, and decrypts the encrypted text. Moreover, when the user's detected fingerprint is verified successfully and the user's instruction requests specifies the encryption of plain text the processing controller encrypts a symmetric key using a public key and associates these keys with the plain text.

The fingerprint apparatus recited in claim 17 includes a fingerprint detection means (111, 112, 113, 114) a fingerprint identification means 120, and a storage-information means 140. The fingerprint identification means 120 verifies fingerprint data detected by said fingerprint detection means (111, 112, 113, 114) with fingerprint data recorded by the storage-information means 140.

VI. ISSUES

The issue presented for appeal in this application is as follows:

1. Whether the Examiner erred in finally rejecting claims 1, 2, 4, 5, 9-11, and 17-19 under 35 U.S.C. §102(a) as anticipated by *Pare Jr. et al.*, U.S. Patent No. 5,838,812.

VII. GROUPING OF CLAIMS

For purposes of this appeal brief only, and without conceding the teachings of any prior art reference, the claims have been grouped as indicated below:

Group Claim(s)

1. Claims 1, 2, 4, and 5 stand or fall together with respect to the §102 rejection over *Pare Jr.*

2. Claims 9-11 stand or fall together with respect to the §102 rejection over *Pare Jr.*

3. Claims 17-19 stand or fall together with respect to the §102 rejection over *Pare Jr.*

In Section VIII below, Applicant has included arguments supporting the separate patentability of each claim group as required by 37 C.F.R. 1.192(c)(7). See, for example, M.P.E.P. § 1206.

VIII. ARGUMENTS

1. In the final Office Action dated May 18, 2004 (Paper No. 13), the following rejections were presented by the Examiner.

(i) 35 U.S.C. §112, first paragraph

None

(ii) 35 U.S.C. §112, second paragraph

None

(iii) 35 U.S.C. §102

Claims 1, 2, 4, 5, 9-11, and 17-19 were rejected under 35 U.S.C. §102(a) as anticipated by *Pare Jr. et al.*, U.S. Patent No. 5,838,812.

(iv) 35 U.S.C. §103

None

(v) Other

None

2. For at least the reasons set forth below, the aforementioned claim rejection is both technically and legally unsound. Accordingly, the §102 rejections should be reversed.

(i) 35 U.S.C. §112, first paragraph

None

(ii) 35 U.S.C. §112, second paragraph

None

(iii) 35 U.S.C. §102

A. Claims 1, 2, 4, and 5 are allowable over the applied art

Independent claim 1 recites an authentication system used when stored information is manipulated, comprising a host computer comprising, input means for inputting a user's instruction; command output means for generating from the user's instruction an instruction command which requests a predetermined processing to be executed and for outputting the instruction command; and communication means for communicating with an external unit; and a fingerprint identification apparatus comprising, communication means for communicating with said host computer; processing control means for executing a predetermined processing according to the instruction command input from said host computer by said communication means; fingerprint detection means for detecting a fingerprint and for generating fingerprint data; storage-information recording means for recording the fingerprint data and storage information related to the fingerprint data; and fingerprint identification means for verifying fingerprint data detected by said fingerprint detection means with the fingerprint data recorded by said storage-information recording means, wherein said storage-information recording means stores a private key generated by the public-key encryption method, wherein said processing control means accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the user's next instruction specifies a decryption of an encrypted text; wherein said processing control means generates a private key, symmetric key, and a public key to encrypt the symmetric key when the user's next instruction specifies an encryption of plain text; and wherein the user's next instruction is sent to the host computer through communication cable.

Pare Jr. discloses a system for identifying individuals for performing financial transactions and non-financial transmissions, which can accommodate a large number of users. In particular, a data processing center 1 connects to various terminals 2 and computer networks 4 through a various types of communication mediums 3. A firewall machine 5 prevents electronic intrusion of the system and a gateway machine 6 executes the requests of the users, and decrypts data received from the various terminals. The various terminals can be any of a number of data entry and biometric devices 13. The terminal 2 communicates to other devices on the network via a conventional modem 18 using request packets 19 and response packets 20. During communication, certain portions of the request packets 19 and response packets 20 are encrypted while other portions of these packets are sealed. Namely,

when sending information to a data processing center 1, the biometric device 13 outputs an encrypted biometric–PIC block that includes a message key. That is, each biometric-PIC block received by the data processing center 1 may also contain an optional response key.

Before responding to a request that includes a response key, the data processing center (DPC) encrypts the reply packet with the response key. When receiving a show response command, a biometric input apparatus (BIA) is instructed to use its current Response Key to decrypt the private code from the system (col. 20, lines 51-57). Moreover, when receiving a decrypt response command, the BIA is instructed to use its current Response Key to decrypt the encrypted portion of the response message (col. 21, lines 37-41). In the discussion of BIA Software command sets (See col. 23, line 22 through col. 25, line 57), *Pare, Jr.* discloses that either the show response command or the decrypt response command is used to decrypt a message. Furthermore, in discussing the operation of an Internet teller terminal (see col. 29, line 62 through col. 30, line 59), *Pare,* Jr. fails to disclose, teach, or suggest at least accessing the generated private key, decrypting a symmetric key, and decrypting the encrypted text using the decrypted symmetric key when the user's next instruction is one that specifies a decryption of an encrypted text. At best, *Pare, Jr.* discloses that the response key is either used to decrypt a private code or used to decrypt the encrypted portion of a response message. Because *Pare, Jr.* fails to disclose, teach or suggest all the elements recited in claim 1, even if the private code as disclosed by *Pare, Jr.* can be interpreted as being analogous to a key, this interpretation still does not render the claimed invention obvious over *Pare, Jr.*

The Office Action alleges that *Pare Jr.* discloses a data encryption standard (DES) encryption library and public key encryption library that generate private key, and perform encryption and decryption processing on text according to the user's instruction. However, as discussed above, the decryption process disclosed by *Pare, Jr.* does not perform the same steps as those recited in claim 1, and therefore does not render the same secure communication as achieved by the claimed invention. In contrast, the claimed invention recites accessing the generated private key, decrypting a symmetric key, and decrypting the encrypted text using the decrypted symmetric key when the user's next instruction is one that specifies a decryption of an encrypted text. This decryption process enables for safe storage of private keys inside the fingerprint apparatus.

To properly anticipate a claim, the document must disclose, explicitly or implicitly, each and every feature recited in the claim. *See* Verdegall Bros. v. Union Oil Co. of Calif., 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). *Pare, Jr.* fails to disclose, teach, or suggest every element recited in claim 1. Accordingly, Appellant respectfully requests that the rejection of claim 1 under §102 not be sustained.

Claims 2, 4, and 5 depend from claim 1. By virtue of this dependency, Appellant submits that claims 2, 4, and 5 are allowable for at least the same reasons given above with respect to claim 1. In addition, Appellant submits that claims 2, 4, and 5 are further distinguished over *Pare, Jr.* by the additional elements recited therein, and particularly with respect to each claimed combination. Appellant respectfully requests, therefore, that the rejection of claims 2, 4, and 5 under 35 U.S.C. §102 not be sustained.

B. Claims 9-11 are allowable over the applied art

Independent claim 9 recites an authentication method used when stored information is manipulated, comprising the steps of a host computer informing a user of a fingerprint-identification request according to a user's instruction and issuing a fingerprint-identification instruction command to a fingerprint identification apparatus; the fingerprint identification apparatus reading a fingerprint after the user places a finger on the fingerprint identification apparatus, verifying the read fingerprint with a stored fingerprint, and sending a fingerprint-identification result to the host computer; the host computer allowing the user to specify the next instruction when the result is affirmative, and issuing the instruction command corresponding to the next instruction; and the fingerprint identification apparatus accessing storage information according to the instruction command and executing a predetermined processing, wherein said storage-information recording means stores a private key generated by the public-key encryption method, and wherein the fingerprint identification apparatus accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the instruction command specifies a decryption of an encrypted text, wherein the fingerprint identification apparatus generates a symmetric key and a public key to encrypt the symmetric key when the instruction command is one that specifies an encryption of plain text, and wherein the instruction command is sent to the host computer through communication cable.

As discussed above, *Pare, Jr.* fails to disclose, teach, or suggest at least accessing the generated private key, decrypting a symmetric key, and decrypting the encrypted text using the decrypted symmetric key when the user's next instruction is one that specifies a decryption of an encrypted text. In contrast, *Pare, Jr.* discloses that when receiving a show response command, a biometric input apparatus (BIA) is instructed to use its current Response Key to decrypt the private code from the system (col. 20, lines 51-57), and when receiving a decrypt response command, the BIA is instructed to use it's current Response Key to decrypt the encrypted portion of the response message (col. 21, lines 37-41). In the discussion of BIA Software command sets (See col. 23, line 22 through col. 25, line 57), *Pare, Jr.* discloses that either the show response command or the decrypt response command is used to decrypt a message.

The claimed invention recites accessing the generated private key, decrypting a symmetric key, and decrypting the encrypted text using the decrypted symmetric key when the user's next instruction is one that specifies a decryption of an encrypted text. This decryption process enables for safe storage of private keys inside the fingerprint apparatus.

To properly anticipate a claim, the document must disclose, explicitly or implicitly, each and every feature recited in the claim. *See* Verdegall Bros. v. Union Oil Co. of Calif., 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). *Pare, Jr.* fails to disclose, teach, or suggest every element recited in claim 9. Accordingly, Appellant respectfully requests that the rejection of claim 9 under §102 not be sustained.

Claims 10 and 11 depend from claim 9. By virtue of this dependency, Appellant submits that claims 10 and 11 are allowable for at least the same reasons given above with respect to claim 1. In addition, Appellant submits that claims 10 and 11 are further distinguished over *Pare, Jr.* by the additional elements recited therein, and particularly with respect to each claimed combination. Appellant respectfully requests, therefore, that the rejection of claims 10 and 11 under 35 U.S.C. §102 not be sustained.

C. Claims 17-19 are allowable over the applied art

Independent claim 17 recites a fingerprint identification apparatus in an authentication system used when stored information is manipulated, comprising communication means for communicating with a host computer; processing control means for executing a predetermined processing according to an instruction command input from

the host computer by said communication means; fingerprint detection means for detecting a fingerprint and for generating fingerprint data; storage-information recording means for recording the fingerprint data and storage information related to the fingerprint data; and fingerprint identification means for verifying fingerprint data detected by said fingerprint detection means with the fingerprint data recorded by said storage-information recording means.

Pare Jr. fails to disclose, teach, or suggest a fingerprint apparatus that includes at least a fingerprint detection means for detecting a fingerprint and for generating fingerprint data and fingerprint identification means for verifying fingerprint data detected by said fingerprint detection means with the fingerprint data recorded by storage-information recording means. In contrast, *Pare Jr.* discloses a system for authorizing a transaction by correlating a user's biometric sample with an authenticated and stored biometric sample, where the correlation of the user's biometric sample with the stored biometric sample is conducted between two separate devices over a network.

The claimed invention recites a fingerprint apparatus that comprises fingerprint detection means and fingerprint identification means. In particular, the fingerprint apparatus is wholly contained within a single integrated unit, whereas the correlation of the biometric sample disclosed by *Pare, Jr.* is conducted between, for example, a biometric input device 12 and a communication terminal 2 over a network. *See* Figure 3.

To properly anticipate a claim, the document must disclose, explicitly or implicitly, each and every feature recited in the claim. *See* Verdegall Bros. v. Union Oil Co. of Calif., 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). *Pare, Jr.* fails to disclose, teach, or suggest every element recited in claim 17. Accordingly, Appellant respectfully requests that the rejection of claim 17 under §102 not be sustained.

Claims 18 and 19 depend from claim 17. By virtue of this dependency, Appellant submits that claims 18 and 19 are allowable for at least the same reasons given above with respect to claim 1. In addition, Appellant submits that claims 18 and 19 are further distinguished over *Pare, Jr.* by the additional elements recited therein, and particularly with respect to each claimed combination. Appellant respectfully requests, therefore, that the rejection of claims 18 and 19 under 35 U.S.C. §102 not be sustained.

IX. CLAIMS INVOLVED IN THE APPEAL

A copy of the claims involved in the present appeal is attached hereto as Appendix A. As indicated above, the claims in Appendix A include the amendments filed by Applicant in the Amendment After Final filed on March 30, 2004.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-0013, under Order No. SON-1710 from which the undersigned is authorized to draw.

Dated: September 1, 2004

Respectfully submitted,

By_____
Ronald P. Kananen
Registration No.: 24,104
Attorney for Applicant

RADER, FISHMAN & GRAUER, PLLC
Lion Building
1233 20th Street, N.W., Suite 501
Washington, D.C. 20036
Tel: (202) 955-3750
Fax: (202) 955-3751
Customer No. 23353

Enclosure(s): Appendix A - Claims 1, 2, 4, 5, 9-11 and 17-19

DC164410

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 09/466,965

1. (PREVIOUSLY PRESENTED) An authentication system used when stored information is manipulated, comprising:

a host computer comprising:

input means for inputting a user's instruction;

command output means for generating from the user's instruction an instruction command which requests a predetermined processing to be executed and for outputting the instruction command; and

communication means for communicating with an external unit; and

a fingerprint identification apparatus comprising:

communication means for communicating with said host computer;

processing control means for executing a predetermined processing according to the instruction command input from said host computer by said communication means;

fingerprint detection means for detecting a fingerprint and for generating fingerprint data;

storage-information recording means for recording the fingerprint data and storage information related to the fingerprint data; and

fingerprint identification means for verifying fingerprint data detected by said fingerprint detection means with the fingerprint data recorded by said storage-information recording means,

wherein said storage-information recording means stores a private key generated by the public-key encryption method,

wherein said processing control means accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the user's instruction specifies a decryption of an encrypted text,

wherein said processing control means generates a symmetric key and a public key to encrypt the symmetric key when the user's instruction specifies an encryption of plain text, and

wherein the user's instruction is sent to the host computer through communication cable.

2. (PREVIOUSLY PRESENTED) The authentication system according to Claim 1, wherein said storage-information recording means allows recorded storage information to be accessed only once immediately after the fingerprint-identification result is affirmative.

3. (CANCELED).

4. (PREVIOUSLY PRESENTED) The authentication system according to Claim 1, wherein said fingerprint identification apparatus further comprises encryption processing means for generating an encryption key, for performing encryption by the use of the encryption key, and for performing decryption.

5. (PREVIOUSLY PRESENTED) The authentication system according to Claim 4, wherein said encryption processing means generates a public key and a private key according to the public-key encryption method, and decrypts an encrypted text by the use of the private key, wherein the encrypted text is received from the host computer and decrypted plain text is sent to the host computer.

6. - 8. (CANCELED).

9. (PREVIOUSLY PRESENTED) An authentication method used when stored information is manipulated, comprising the steps of:

a host computer informing a user of a fingerprint-identification request according to a user's instruction and issuing a fingerprint-identification instruction command to a fingerprint identification apparatus;

the fingerprint identification apparatus reading a fingerprint after the user places a finger on the fingerprint identification apparatus, verifying the read fingerprint with a stored fingerprint, and sending a fingerprint-identification result to the host computer;

the host computer allowing the user to specify the next instruction when the result is affirmative, and issuing the instruction command corresponding to the next instruction; and

the fingerprint identification apparatus accessing storage information according to the instruction command and executing a predetermined processing,

wherein said storage-information recording means stores a private key generated by the public-key encryption method, and

wherein the fingerprint identification apparatus accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the instruction command specifies a decryption of an encrypted text,

wherein the fingerprint identification apparatus generates a symmetric key and a public key to encrypt the symmetric key when the instruction command is one that specifies an encryption of plain text, and

wherein the instruction command is sent to the host computer through communication cable.

10. (PREVIOUSLY PRESENTED) The authentication method according to Claim 9, wherein, in the step of the fingerprint identification apparatus accessing the storage information according to the instruction command and executing a predetermined processing, the storage information is allowed to be accessed only once immediately after the fingerprint-identification result is affirmative.

11. (PREVIOUSLY PRESENTED) The authentication method according to Claim 9, wherein the storage information includes a private key generated by the public-key encryption method, and in the step of the fingerprint identification apparatus accessing the storage information according to the instruction command and executing a predetermined processing, a predetermined encrypted text is decrypted by the use of the private key, wherein the encrypted text is received from the host computer and decrypted plain text is sent to the host computer.

12. - 16. (CANCELED).

17. (PREVIOUSLY PRESENTED) A fingerprint identification apparatus in an authentication system used when stored information is manipulated, comprising:

communication means for communicating with a host computer;

processing control means for executing a predetermined processing according to an instruction command input from the host computer by said communication means;

fingerprint detection means for detecting a fingerprint and for generating fingerprint data;

storage-information recording means for recording the fingerprint data and storage information related to the fingerprint data; and

fingerprint identification means for verifying fingerprint data detected by said fingerprint detection means with the fingerprint data recorded by said storage-information recording means.

18. (PREVIOUSLY PRESENTED) A fingerprint identification apparatus according to Claim 17, wherein said storage-information recording means allows recorded storage information to be accessed only once immediately after the fingerprint-identification result is affirmative.

19. (PREVIOUSLY PRESENTED) A fingerprint identification apparatus according to Claim 17, wherein said fingerprint identification apparatus further comprises encryption processing means for generating an encryption key, for performing encryption by the use of the encryption key, and for performing decryption.